



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/396,054 | 09/15/1999 | YOSHIHITO ISHIBASHI | 450100-02090 | 6914 |

20999 7590 07/16/2004
FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER

ABEL JALIL, NEVEEN

| ART UNIT | PAPER NUMBER |
|----------|--------------|
|----------|--------------|

2175

13

DATE MAILED: 07/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/396,054

Applicant(s)

ISHIBASHI, YOSHIHITO

Examiner

Neveen Abel-Jalil

Art Unit

2175

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 June 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


DOV POPOVICH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1-June -2004 has been entered.
2. The amendment filed on 1-June-2004 has been received and entered. Claims 1-41 are pending

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1-15, and 19-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Saito (U.S. Patent No. 6,741,991 B2).

As to claim 1, Saito discloses a content management method for a data storage provided with a plurality of content storing means, comprising the steps of:

storing a content key encrypted with a first storage key in a first content storing means, and storing along with said content key encrypted with the first storage key a content encrypted with the content key (See column 7, lines 8-15);

decrypting the encrypted content key with the first storage key (See column 7, lines 16-44); and

encrypting the content key obtained by the above decryption with a newly generated second storage key (See column 7, lines 16-44); and

storing the content key encrypted with the second storage key along with the encrypted content in a second content storing means (See column 7, lines 50-67).

As to claim 2, Saito discloses wherein the second storage key is generated based on a random number (See column 6, lines 45-48).

As to claim 3, Saito discloses wherein the content key obtained by the decryption is encrypted with identification information of the second content storing means and stored into the second content storing means (See column 6, lines 49-67).

As to claim 4, Saito discloses wherein the content key is encrypted, in the first content storing means, with the first storage key and identification information of the first content storing means, and the content key stored in the first content storing means is decrypted with the first storage key and identification information of the first content storing means (See column 4, lines 30-67).

As to claim 5, Saito discloses wherein the second storage key is generated by a decrypted key generating means provided in the data storage (See column 8, lines 43-67).

As to claim 6, Saito discloses wherein the second storage key is encrypted with a public key for a key management unit for management of the storage keys to generate a third storage key and the third storage key is stored into the second content storing means (See column 10, lines 6-45, also see column 16, lines 39-67).

As to claim 7, Saito discloses wherein the data storage deletes the second storage key depending upon whether the third storage key has been stored in the second content storing means (See column 9, lines 23-49).

As to claim 8, Saito discloses wherein when decrypting the content key stored in the second content storing means, the data storage sends the third storage key to the key management unit; and the key management unit generates a second storage key based on the third storage key while accounting the data service following a predetermined procedure (See column 16, lines 31-67).

As to claim 9, Saito discloses wherein the second storage key is generated by a storage key generating means provided in the key management unit which manages the storage keys; and the key management unit has stored therein the second storage key and the identification information of the second content storing means in which the content key encrypted with the above generated second storage key (See column 11, lines 5-67).

As to claim 10, Saito discloses wherein upon the generation of the second storage key, the key management unit accounts the data service following the predetermined procedure (See column 19, lines 19-55, wherein “accounts” reads on “escrow”).

As to claim 11, Saito discloses wherein the key management encrypts the second storage key with the management key to generate a third storage key, and sends the third storage key to the data storage (See column 19, lines 19-55); and

the data storage stores the received third storage key into the second content storing means (See column 19, lines 19-55).

As to claim 12, Saito discloses wherein the data storage deletes the second storage key depending upon whether the third storage key has been stored in the second content storing means (See column 19, lines 45-47, wherein “deletes” reads on “abandoned”).

As to claim 13, Saito discloses wherein the key management unit has stored therein the identification information of the second content storing means in which the content key encrypted with the second storage key (See column 32, lines 40-67, also see column 33, lines 1-21);

the data storage sends, when decrypting the content key stored in the second content storing means, the identification information of the second content storing means to the key management unit (See column 32, lines 40-67, also see column 33, lines 1-21); and

the key management unit generates a second storage key based on the result of comparison between the identification information of the second content storing means, send from the data storage, and the identification information of the second content storing means, held in the key management unit itself, while accounting the data service following the predetermined procedure (See column 32, lines 40-67, also see column 33, lines 1-21).

As to claim 14, Saito discloses wherein the second content storing means has stored therein the identification information of the data storage (See column 6, lines 40-56).

As to claim 15, Saito discloses wherein the data storage starts decrypting the content key stored in the second content storing means depending upon the result of an inspection of the

identification information of the data storage, stored in the second content storing means (See column 10, lines 10-45).

As to claim 19, Saito discloses wherein the content key stored in the first content storing means is stored along with the identification information of the first content storing means into the second content storing means (See column 6, lines 30-67);

the identification information stored in the second content storing means is stored into the data storage when the content key stored in the second content storing means is decrypted (See column 6, lines 30-67); and

the data storage makes, when a request is made to decrypt the content key in the first content storing means, an error process based on the result of comparison between the identification information of the first content storing means in consideration and the identification information of the second content storing means (See column 7, lines 1-67).

As to claim 20, Saito discloses a content storage system, comprising:

a first content storing means having stored therein a content key encrypted with a first storage key and a content encrypted with the content key (See column 12, lines 1-65, also see column 11, lines 31-40);

means for decrypting key data (See column 10, lines 57-67);

means for encrypting key data (See column 5, lines 49-52);

means for generating a storage key (See column 6, lines 57-65);

a second content storing means for storing an encrypted content key obtained by encrypting, in the encrypting means, the content key obtained by decryption with the first storage key in the decrypting means, using the second storage key generated by the storage key generating means, and the encrypted content (See column 12, lines 1-65); and
means for storing the storage keys (See column 12, lines 1-18).

As to claim 21, Saito discloses wherein the storage key storing means generates the second storage key by means of a random number generator (See column 6, lines 44-48).

As to claim 22, Saito discloses wherein a content key obtained by encrypting, in the encrypting means, the content key obtained by the decryption in the decrypting means, with the first storage key and identification information of the second content storing means, is stored in the second content storing means (See column 6, lines 49-67, and see column 7, lines 1-67).

As to claim 23, Saito discloses wherein the content key is encrypted, in the first content storing means, with the first storage key and identification information of the first content storing means; and the content key stored in the first content storing means is decrypted with the first storage key and identification information of the first content storing means (See column 6, lines 49-67, and see column 7, lines 1-67).

As to claim 24, Saito discloses wherein the first content storing means, decrypting means, encrypting means, second content storing means, storage key storing means and storage key

generating means form together a data storage (See column 30, lines 16-48); and further comprising a key management unit which manages the storage keys of the data storage (See column 10, lines 6-56).

As to claim 25, Saito discloses wherein the data storage is a data receiver which receives a content encrypted and sent from a data transmitter (See column 5, lines 13-40).

As to claim 26, Saito discloses comprising means for storing the public key of the key management unit; and wherein the second content storing means has stored therein the second storage key along with a third storage key obtained by encrypting the second storage key with the public key (See column 22, lines 52-67, also see column 23, lines 1-5).

As to claim 27, Saito discloses wherein the data storage deletes the second storage key depending upon whether the third storage key is stored in the second content storing means (See column 19, lines 45-47, wherein “deletes” reads on “abandoned”).

As to claim 28, Saito discloses wherein when decrypting the content key stored in the second content storing means, the data storage sends the third storage key to the key management unit (See column 19, lines 33-47); and the key management unit sends a second storage key generated based on the third storage key to the data transmitter while accounting the data service following a predetermined procedure (See column 21, lines 6-28).

As to claim 29, Saito discloses wherein the second content storing means has stored therein the identification information of the data storage (See column 6, lines 32-67, and see column 10, lines 10-31).

As to claim 30, Saito discloses wherein the data storage starts decrypting the content key stored in the second content storing means depending on the result of inspection of the identification information of the data storage, stored in the second content storing means (See column 22, lines 5-51).

As to claim 31, Saito discloses wherein the first content storing means, decrypting means, encrypting means, second content storing means and storage key storing means form together a data storage (See column 22, lines 20-50); and

comprising the storage key generating means and further a key management unit which manages the storage keys of the data storage (See column 22, lines 5-20).

As to claim 32, Saito discloses wherein the data storage is a data receiver which receives a content encrypted and sent from a data transmitter (See column 5, lines 13-40).

As to claim 33, Saito discloses wherein the key management unit comprises an identification information storing means in which the storage key generated by the key management unit and the identification information of the content storing means in which the content key encrypted with the generated storage key (See column 24, lines 43-55).

As to claim 34, Saito discloses wherein the key management unit accounts the data service following the predetermined procedure depending upon the generation of the storage key (See column 4, lines 16-34).

As to claim 35, Saito discloses wherein the key management unit comprises means for storing storage keys;

the key management unit generates a third storage key by decrypting the second storage key with the storage key and sends it to the data storage (See column 22, lines 52-67); and

the data storage stores the third storage key into the second content storing means (See column 23, lines 1-5).

As to claim 36, Saito discloses wherein the data storage deletes the second storage key depending upon whether the third storage key is stored into the second content storing means (See column 7, lines 10-41).

As to claim 37, Saito discloses wherein the key management unit comprises means for storing the second storage key and the identification information of the second content storing means in which the content key encrypted with the second storage key is stored (See column 6, lines 39-67);

the key management unit accounts, when the data storage decrypts the content key, the data service following the predetermined procedure based on the result of comparison (See

abstract) between the identification information of the second content storing means, sent from the data storage, and the identification information stored in the identification information storing means (See column 7, lines 37-67).

As to claim 38, Saito discloses wherein the second content storing means has stored therein the identification information of the data storage (See column 7, lines 37-65).

As to claim 39, Saito discloses wherein the data storage starts decrypting the content key stored in the second content storing means (See column 6, lines 45-65).

As to claim 40, Saito discloses wherein the content key obtained by decryption from the second content storing means has added thereto information that the content key is a one obtained by restoration, as requirement information (See column 13, lines 26-40).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 16-18, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito (U.S. Patent No. 6,741,991 B2) in view of Takashima et al. (U.S. Patent No. 5,701,343).

As to claim 16, Saito does not teach wherein the decrypted content key supplied from the second content storing means has added thereto information that the content key is a one obtained by restoration.

Takashima et al. teaches wherein the decrypted content key supplied from the second content storing means has added thereto information that the content key is a one obtained by restoration (See column 8, lines 13-65).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to have modified Saito to include wherein the decrypted content key supplied from the second content storing means has added thereto information that the content key is a one obtained by restoration.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Saito by the teaching of Takashima et al. to include wherein the decrypted content key supplied from the second content storing means has added thereto information that the content key is a one obtained by restoration because it provides security and consistency.

As to claim 17, Saito as modified discloses wherein when moving the content key having added thereto the information that the content key is a restored one, the data storage makes an error process based on the result of comparison between the content key and a content key stored in a destination to which the content key is to be moved (See Takashima et al. column 15, lines 42-67).

As to claim 18, Saito does not teach wherein the content key has added thereto frequency information which limits the number of times the content key can be used.

Takashima et al. teaches wherein the content key has added thereto frequency information which limits the number of times the content key can be used (See column 8, lines 13-65).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to have modified Saito to include wherein the content key has added thereto frequency information which limits the number of times the content key can be used.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Saito by the teaching of Takashima et al. to include wherein the content key has added thereto frequency information which limits the number of times the content key can be used because it provides security and consistency.

As to claim 41, Saito does not teach wherein the content key has added thereto frequency information which limits the number of times the content key can be used.

Takashima et al. teaches wherein the content key has added thereto frequency information which limits the number of times the content key can be used (See column 8, lines 13-65).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to have modified Saito to include wherein the content key has

added thereto frequency information which limits the number of times the content key can be used.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Saito by the teaching of Takashima et al. to include wherein the content key has added thereto frequency information which limits the number of times the content key can be used because it provides security and consistency.

Response to Arguments

7. Applicant's arguments with respect to claims 1-41 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Tatebayashi et al. (U.S. Patent No. 6,028,937) teaches two-way encryption authentication in challenge response format.


9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Neveen Abel-Jalil whose telephone number is 703-305-8114.

The examiner can normally be reached on 8:30AM-5:30PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on 703-305-3830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Neveen Abel-Jalil
July 8, 2004



DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100